reference. Shwed would still not disclose "policy data containing rules defining relevant commercial data" as specified in claim 1. The rules in Shwed define the packets themselves only in terms of destination, sender addresses and service type, and not in terms of any relevant commercial data.

Additionally, an interpretation of the packets as relevant commercial data would mean that the modifying or logging of the packets be relevant commercially, and yet the only need to stop packets disclosed in Shwed is security. There is therefore no storage of relevant commercial data. Furthermore, no description is given in Shwed of what logging a packet on the system entails. It could just be an entry that a packet was detected and modified, rather than the packet itself.

Claim 1 and its dependent claims 2-23 are therefore patentable over Shwed.

More particularly, with respect to dependent claim 9, the Examiner states that Shwed discloses the identification of digital certificates, and that these are stored in the data repository. However, Shwed does not disclose or suggest identification or storage of digital certificates.

The portion of the Shwed abstract referred to by the Examiner states that an accepted packet may be modified by encryption, decryption, signature generation, or signature verification. Nowhere does Shwed specify that digital certificates from a plurality of inbound or outbound workstations are identified and stored in a data repository. If any digital certificates are stored in Shwed, they would likely be stored locally on the workstation where they could be used, rather than being transmitted across the network to a system administrator to whom they would have little or no relevance. In accordance with claim 9, digital certificates and/or said descriptive data identifying digital certificates are stored in a data repository. This avoids the need to store such certificates locally causing repetition and an uneconomic use of resources.

Indeed, the use of the system administrator's storage device 212 is barely discussed in Shwed. The abstract only mentions the packet related events can be logged. This is explained further at column 9, lines 21 to 26, which state:

> [T]he packet is compared with the security rule, and a determination is made as to whether or not the packet matches the rule. If the packet matches the rule, it may be logged on the

> system administrator's log, and if an illegal attempt has been made to enter the system, an alert may be issued.

Thus, there is no disclosure of storing relevant commercial data comprising digital certificates in a data repository.

Independent claim 24 is directed to a method of managing information. The claim specifies identifying in at least one of said outbound data and said inbound data, relevant commercial data that is to be stored in said data repository in accordance with said rules in said policy data; and storing said relevant commercial data in said data repository. These steps are neither disclosed, nor suggested by Shwed. Claim 24 and its dependent claims 25-46 are therefore patentable over Shwed.

Independent claim 438 is directed to an information management system that includes analyzing means, operable in conjunction with said policy means, for monitoring at least one of said outbound data and said inbound data, identifying in at least one of said outbound data and said inbound data, relevant commercial data that is to be stored in said storage means in accordance with said rules in said policy means, and causing said relevant commercial data to be stored in said storage means. These elements are neither disclosed, nor suggested by Shwed. Claim 438 and its dependent claims 439-460 are therefore patentable over Shwed.

II. Independent claims 114, 136, and 476 and their respective dependent claims

None of these claims were addressed in the office action.

Independent claim 114 is directed to an information management system that includes an analyser operable in conjunction with policy data to monitor outbound data from a workstation and to determine, in accordance with said rules in said policy data, an appropriate encryption strength for the outbound data; wherein said analyser controls transmission of said outbound data from said application in dependence upon said determination of an appropriate encryption strength.

These elements are neither disclosed, nor suggested by Shwed. Shwed discusses (e.g., from column 12, line 65 onwards) applying encryption to the data to be transmitted between firewalls. However the method for determining the encryption to be used, comprises the normal

negotiation between sender and transmitter and does not include determining the strength with reference to the policy data.

Additionally, the encryption in Shwed depends only on the source, destination or service type, not the content of the data. See, e.g., column 13, lines 13-16, which provides:

> For encryption, for example, to occur a rule in the rule base must explicitly call for encryption to occur on packets which have a particular source, destination, and service type.

Claim 114 and its dependent claims 115-135 are thus patentable over Shwed.

Independent claim 136 is directed to a method of managing information, which includes the steps of: analysing said outbound data to determine, in accordance with said rules in said policy data, an appropriate encryption strength for the outbound data; and controlling transmission of said outbound data from said application in dependence upon the determination of an appropriate encryption strength in said analysing step. These steps are neither disclosed, nor suggested by Shwed. Claim 136 and dependent claims 137-157 are thus patentable over Shwed.

Independent claim 476 is directed to an information management system that includes analyzing means, operable in conjunction with said policy data, for monitoring said outbound data to determine, in accordance with said rules in said policy data, an appropriate encryption strength for the outbound data; wherein said analyzing means controls transmission of said outbound data from said application means in dependence upon said determination of an appropriate encryption strength. Shwed neither discloses, nor suggests the claimed analyzing means. Independent claim 476 and dependent claims 477-497 are thus patentable over Shwed.

III. Independent claims 178, 220, and 498 and their respective dependent claims

None of these claims were addressed in the office action.

Independent claim 178 is directed to an information management system that includes an analyser operable in conjunction with said policy data to analyse at least one of said outbound data and said inbound data, to identify the existence of a commercial transaction occurring

between a client workstation and a third party by analysing said outbound or said inbound data, and to cause transaction data that is all or part of said outbound data or said inbound data related to an identified commercial transaction to be stored in said data repository.

The system can thereby, e.g., identify and store online transactions as they occur, providing a valuable record of data, e.g., for accounting and audit purposes. Such a system is not disclosed or suggested by Shwed. Shwed merely mentions comparing received packets of data to a rule defined in terms of the source, destination, or service type of a data packet. Thus, there is no identification of commercial transaction data, much less relating to a commercial transaction occurring between a client workstation and a third party.

Furthermore, although column 9, lines 23-27 of Shwed specify that "if a packet matches a security rule, it may be logged on the system administrators log", this cannot be viewed as causing "transaction data that is all or part of the said outbound data or said inbound data related to an identified commercial transaction" to be stored.

Shwed is concerned with the trapping of attacks against the network. The packet that is logged is therefore clearly one which is found suspect when matched against a security rule. As described in col. 9, line 24, "if an illegal attempt has been made to enter the system, an alert may be issued."

Claim 178 and dependent claims 179-219 are thus patentable over Shwed.

Independent claim 220 is directed to a method of managing information. The method features the steps of analysing, at least one of said outbound data and said inbound data to identify, with reference to said rules of said policy data, the existence of a commercial transaction occurring between a client workstation and a third party; and storing transaction data that is all or part of said outbound data or said inbound data related to an identified commercial transaction in said data repository. Shwed does not disclose or suggest these steps. Claim 220 and dependent claims 221-261 are thus patentable over Shwed.

Independent claim 498 is directed to an information management system that includes analyzing means, operable in conjunction with said policy data, for analyzing at least one of said outbound data and said inbound data, to identify the existence of a commercial transaction occurring between a client workstation and a third party, and for causing transaction data that is all or part of said outbound data or said inbound data related to an identified commercial

transaction to be stored in said storage means. Shwed does not disclose or suggest the claimed system. Claim 498 and dependent claims 499-539 are thus patentable over Shwed.

IV. Independent claims 304, 329, and 540 and their respective dependent claims

None of these claims were addressed in the office action.

Independent claim 304 is directed to an information management system that includes an analyser operable in conjunction with said policy data to identify in at least said outbound data, transaction data that may be part of a transaction, and to make a determination in accordance with said rules of said policy data as to whether the transmission of said transaction data would satisfy said rules; and wherein the transmission of said transaction data by said application is dependent on said determination made by said analyser.

The claim requires that the analyzer identify in at least said outbound data, data that may be part of a transaction, and to determine whether the transmission of the transaction data would satisfy the policy rules. As a non-limiting example, the system is able to allow the commercial transactions of a plurality of users to be managed centrally, allowing a financial director, say, to review transactions before they occur, or even possibly to prevent them.

Shwed in no way discloses or suggests a system in which commercial transactions are identified. It therefore has no rule for identifying transaction data, and as mentioned above is only concerned with the security of a messaging system.

Independent claim 329 is directed to a method for managing information. The method features the steps of analysing at least said outbound data to identify, with reference to said rule of said policy data, transaction data that may be part of a transaction; determining, in accordance with said rules of said policy data, whether the transmission of said transaction data would satisfy said rules; and controlling transmission of said transaction data by said application in dependence on the determination made in said determining step. These steps are neither disclosed, nor suggested by Shwed. Claims 329 and dependent claims 330-353 are patentable over Shwed.

Independent claim 540 is directed to an information management system that includes analyzer means, operable in conjunction with said policy data, for identifying in at least said

outbound data, transaction data that may be part of a transaction, and for determining, in accordance with said rules of said policy data, whether the transmission of said transaction data would satisfy said rules; and wherein the transmission of said transaction data by said application means is dependent on said determination made by said analyzing means. Shwed does not disclose or suggest the claimed system. Claim 540 and dependent claims 541-564 are thus patentable over Shwed.

V. Independent claims 377, 398, and 565 and their respective dependent claims

None of these claims were addressed in the office action.

Independent claim 377 is directed to an information management system that includes an analyser operable in conjunction with said application to monitor said inbound data and to identify in at least said inbound data, signed data that has been digitally signed with a digital certificate, to extract one or more details of said signed data and to determine whether or not verification is required for said digital certificate. The system also includes policy data, accessible by said analyser, containing rules which define whether or not verification is required for said digital certificate. The analyser determines whether or not verification is required for said digital certificate in dependence on said rules of said policy data and in dependence on said one or more details of said signed data extracted by said analyser.

Shwed is only concerned with the security of a network. The reference does not mention digital certificates, much less any functionality to manage how and when their authenticity is to be verified. Claim 377 and dependent claims 378-397 are patentable over Shwed.

Independent claim 398 is directed to a method of managing information featuring the steps of:

identifying in at least said inbound data, signed data that has been digitally signed with a digital certificate;

extracting one or more details of said signed data; and

determining whether or not verification is required for said digital certificate in dependence on said rules of said policy data and in dependence on said one or more details of said signed data extracted in said extracting step.